IN THE MATTER OF THE SEARCH CERTAIN PROPERTY LOCATED AT THE OFFICE OF HOMELAND SECURITY INVESTIGATIONS 40 SOUTH GAY STREET BALTIMORE, MARYLAND 21202

Case No. 17-2668 BPG

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Augustus Aquino, (sometimes referred to herein as your Affiant) being duly sworn depose and say that:

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI), and formerly known as the United States Customs Service. I am currently assigned to the Office of the Special Agent in Charge in Baltimore, Maryland. I have been so employed since June 1991. As part of my daily duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251 and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256)[1] in all forms of media including computer media. I have also participated in the execution of search warrants, which involved child exploitation and/or child pornography offenses. I am currently assigned to the Maryland Internet Crimes Against Children Task Force (ICAC) which is administered by the

[1] "Child Pornography means any visual depiction, including any photograph, film, video, picture, or computer or computergenerated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . [or] (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct." For conduct occurring after April 30, 2003, the definition also includes "(B) such visual depiction is a digital image, computer image, or computergenerated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct." 18 U.S.C. § 2256(8).

Maryland State Police. The ICAC task force was formed to combat the online exploitation of children in the State of Maryland.

2. I have received formal training from U.S. Customs and HSI and other agencies in the area of child pornography, pedophile behavior, collectors of other obscene material and Internet crime.

3. As a federal agent, your Affiant is authorized to investigate violations of laws of the United States and is a law enforcement officer with the authority to affect arrests and execute warrants issued under the authority of the United States.

4. This affidavit is being submitted in support of a search warrant for the computers, hard drives, a cell phone and removable computer media (more particularly described in Attachment A) currently located at the offices of U.S. Department of Homeland Security, Homeland Security Investigations (HSI), 40 South Gay Street, Baltimore, Maryland 21202. The computers, along with hard drives, cell phone and media were seized on August 9, 2017, pursuant to a state search warrant executed at 50 North Drive, Earleville, Maryland (hereinafter the "SUBJECT PREMISES") and issued by the Honorable Wayne A. Brooks, Judge for the District Court of Howard County, Maryland. A copy of this search warrant is attached and incorporated as **Exhibit A**. The computers, cell phone, external hard drives and other removable media were seized from the SUBJECT PREMISES from the resident identified as Jason Allen MARSH.

5. Your affiant has probable cause to believe the computers, hard drives, cell phone and other removable computer media contain evidence of violations of Title 18 U.S.C Section 2252A(a)(2) (distribution and receipt of child pornography) and Title 18 U.S.C. Section

2252A(a)(5)(B) (possession of child pornography).

6. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of the aforementioned federal statutes are located within the computers, hard drives, digital camera and removable computer media currently held at the offices of HSI and seized from the SUBJECT PREMISES.
The information contained in this affidavit came from my own participation in the inquiry described herein, as well as from other law enforcement officers, including Maryland State Police Troopers and other third parties in each instance I have identified the sources of information upon which I have relied.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

7. Based upon your Affiant's experience in child exploitation investigations and upon information provided to your Affiant by other law enforcement officers, the following can be true of child molesters/child pornographers:

a. Individuals involved in the sexual exploitation of children through child pornography rarely, if ever, dispose of their sexually explicit material, especially when they are used in the seduction of children. The individual procurers of the sexual exploitation materials treat those materials as prized possessions and trophies. It is further unlikely that the condition of those items depicting the sexual exploitation of children will be altered or damaged from the

original condition at the time of receipt based on the desire to keep the items in their original condition. Moreover, taken together, the increased sense of security which a computer affords and the known desire to retain child pornography for long periods provide probable cause to believe that computer images will be retained for as long as other types of child pornography and obscene materials if not longer.

b. Individuals who traffic in child pornography may collect, read, copy or maintain numbers or lists of persons who have similar sexual interests. Individuals involved with the production of child pornography may engage in the trading of images with other like-minded individuals, sending the images they have produced to others in exchange for money or the promise of images of child pornography in return. These contacts are maintained as a means of personal referral, exchange and commercial profit. These names may be maintained in the original publication or mode of receipt, or in files maintained on the computer.

c. Child pornography, or recorded data relating to its transmission, receipt, or distribution that are stored in computer data format, that have been deleted to defeat law enforcement evidence collection efforts, can be recovered by various methods during a forensic examination of the computer system.

FACTS AND CIRCUMSTANCES OF THE INVESTIGATION

8. In May 2017, The Maryland State Police ICAC received information from the ICAC Commanders meeting regarding a joint operation between FBI and ICAC to identify individuals using P2P, specifically eMule, to trade child pornography worldwide. Each user on the eMule is assigned a unique client user hash. At that time an eMule client user hash was provided to the Maryland ICAC along with an IP address. Specific to the instant case, the eMule

client user hash was 438420FDBA0EFE34B2D54A287D9C6F98 and was geolocated to the Elkton, Maryland area. Maryland State Police Corporal Roger Schwarb provided the client user hash and IP address to Baltimore County Detective Josh Rees in an attempt to determine if the eMule client user and/or the IP address was sharing files of interest on the eMule network. Detective Rees was able to associate an IP address, 73.172.75.178 with the eMule client user hash, 438420FDBA0EFE34B2D54A287D9C6F98, the same client user hash provided to him by the Maryland ICAC. Detective Rees connected directly to the IP address 73.172.75.178 and during the period between June 5, 2017 and June 26, 2017, Detective Rees downloaded 181 files of suspected child pornography. By way of example, your affiant has provided descriptions of several of the files downloaded by Detective Rees during this time period. The descriptions are listed below:

> June 6, 2017 – babyshihelpless017.jpg – depicts a male on his knees with an erect penis. In front of the nude male is a nude female toddler who appears to be 2-3 years of age and is bound with black straps. The minor is leaning over an object that appears to be an ottoman which is covered by a green towel. There appears to be sperm on the buttocks of the toddler.
>
> June7, 2017 – 2 8Yrs Olds Molest Drunk Dad.avi – the video is a partial download and depicts two nude minor females standing over an adult male who is wearing jeans and lying on his back. The minors remove the males jeans and masturbate the male.
>
> June 8, 2017 – Baby_Lexxa_licky.avi – this video depicts prepubescent minor female lying on her back with an adult male genitals inserted in the minors mouth. The minor's eyes are blacked out in the video.

9. On July 1, 2017, Detective Rees noted eMule Client User Hash 438420FDBA0EFE34B2D54A287D9C6F98 was now associated with another IP address

76.100.134.76. During the period between July 1, 2017 and July 24, 2017, Detective Rees was able to connect directly to IP address 76.100.134.76. During that time period Detective Rees was able to download 187 files of suspected child pornography from IP address 76.100.134.76. By way of example, descriptions of several of the images and videos downloaded by Detective Rees are listed below.

> July 6, 2017 2011 Pthc Falko Awesome 7Yo And 8Yo Child Porn (99).jpg Depicts two nude prepubescent minor females performing oral sex upon each other and an adult female is in the background in underwear and is placing a dog leash on one of the minor's backs.
>
> July 19, 2017 2011 Falko Awesome 7 and 8 Porn (114).jpg – depicts a prepubescent minor female sitting in the lap of an adult male. The adult male's genitals are against the buttocks of the minor and the adult is holding the minor's legs apart. Both the minor and the adult are facing the camera and the minor is wearing black stockings.
>
> July 19, 2017 – 2010 pthc falko 01(recorded for mobilephone)3pg.avi – This video is approximately 27 minutes and 34 seconds in length. The video depicts adult female inserting a sex toy in the vagina of a prepubescent minor female. The video changes and a prepubescent minor female is digitally penetrating the vagina of an adult female. The video then depicts the minor female handcuffed and an adult male is masturbating the minor with sex toy. The minor is also being digitally penetrated into her anus. The video ends depicting the adult male and female watching pornography and masturbating the minor female.

10. Corporal Schwarb checked the IP addresses 76.100.134.76 and 73.172.75.178, associated with the eMule client user hash 438420FDBA0EFE34B2D54A287D9C6F98 and the downloaded child pornography and determined they were assigned to Comcast Cable Communications. Corporal Schwarb caused a subpoena to be issued to Comcast for the dates and times, Detective Rees had downloaded the above described images and video files. On July 29, 2017, Comcast responded and advised both of the IP addresses were assigned to James

Marsh, 50 North Drive, Earleville, Maryland 21919 during the dates and times of the downloads.

11. On August 9, 2017, Maryland State Police, ICAC assisted by HSI Special Agents executed a state search warrant at the residence located at 50 North Drive, Earlesville, Maryland 21219. A copy of this search warrant is attached and incorporated as **Exhibit A**. The search warrant authorized the search and seizure of digital electronic devices, including computers and computer peripheral devices. Several individuals were identified as currently living at the residence including Xxxxxx Xxxxxx and his wife Xxxxxxx as well as their adult son Jason Allen MARSH.

12. During the execution of the search warrant, your Affiant and Corporal Schwarb interviewed Jason MARSH. After having been read his Miranda Warnings, MARSH waived his Miranda and agreed to speak to your affiant and Corporal Schwarb. During the interview, MARSH admitted to obtaining child pornography via eMule. MARSH claimed to have blocked the file sharing feature on eMule and was just downloading files. MARSH advised he lets the eMule program run constantly and masturbates to the child pornography approximately twice per week. MARSH also admitted he had been a registered sex offender and that his registration stemmed from a case in which he had been accused of sexual abuse of two minors in 1998. MARSH stated he was incarcerated for two and half years, on probation for five years and was on the sex offender registry for longer than he was supposed to be and was eventually removed from the registry. MARSH admitted to looking at child pornography for at least the last 6-7 years. MARSH stated while on probation he was never asked by anyone to examine his computer but that child pornography would probably have been found on his computer. MARSH

admitted to downloading child pornography to disk and there may be as many as 100 DVDs with child pornography. MARSH stated there are several folders on the computer that contain child pornography. When asked about whether or not he remembered videos containing the terms "falko" and "6yo" he said "yes". At several points in the interview, MARSH stated he knew he had a problem and that the 2 ½ years he was incarcerated "helped" but "not enough". MARSH stated he had the impulse to view child pornography but denied ever having the desire to act out and do what was being done to children in the images and videos. MARSH voluntarily agreed to a polygraph examination. However after being transported to the Maryland State Police Barracks he decided not to take the polygraph examination. MARSH was subsequently charged by the Maryland State Police on August 9, 2017 for violations of distribution and possession of child pornography.

13. On August 9, 2017, also during the execution of the search warrant, Trooper First Class (TFC) Joshua Brooks and S/A Jason Shaver CFA conducted an on scene forensic preview of the computer located in Jason MARSH's bedroom in the residence located at 50 North Drive, Earlesville, Maryland. During the forensic preview, TFC Brooks observed the eMule and eMule6.0 folders in the "All Programs" under the Start Menu. The task bar indicated the eMule program was running, but the program was minimized. TFC Brooks observed multiple downloads were completed, partially completed or in the process of downloading. TFC Brooks observed some of the file names downloaded or in the process of downloading were: "TvgLittle Girl Slave – 10 Yo –Bondag…", "Pthc 2010 5Yo Kathie Making Poop Ana…", "piss over baby toddler girl nudej52m…", "pedo rape PERVERTED MANIAC ABUS…" and "Pthc 2012 8Yo

Gorgeous Little Brunett....". TFC Brooks observed in the "Shared Files Tab" several files such as, "Yami 3Yo Cock and Pussy.avi" and "webcam My 9Yo Little SisterNewh...". TFC Brooks then shut down the computer and conducted a forensic preview of the hard drives contained in the computer. During the forensic preview, TFC Brooks located numerous suspected child pornography files including one titled "2011 Pthc falko Awesome 7Yo and 8Yo Child Porn(99).jpg". TFC Brooks also located the file "2011 falko Awesome 7 and 8 Porn(114).jpg". These files were located on the Compaq computer's hard drive seized from the SUBJECT PREMISES and where contained in an eMule folder entitled "Incoming". These files are the same files that were downloaded by Detective Rees on July 6, 2017 and July 19, 2017 and are particularly described in Paragraph 9 of this affidavit. In addition to the computer and hard drives located and previewed several DVDs/CDs were previewed on scene and found to contain child pornography. An example of files contained on the DVDs/CDs and previewed on scene is listed below:

> (PTHC) 6 YO Babyj.mpg – video depicts an adult male performing oral sex upon a prepubescent minor female and then the adult male performs vaginal intercourse upon the minor and ejaculates.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

14. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. I also know that digital devices such as the Compaq Presario Computer, hard drives, cell phone and DVDs/CDs seized from MARSH's residence can be attached or installed to almost any other device with including any other computers to transfer data. Your affiant also knows that data, including videos and images can

be transferred from other devices such as computers, other hard drives, DVDs/CDs seized from MARSH's residence.

15. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the electronic devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the electronic devices that are the subject of this warrant because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, transferred to another device and show a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed

along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the electronic device and the application of knowledge about how an electronic device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to produce child pornography, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

16. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the electronic devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

17-2668 BPG

17. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion into a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

18. Based on the foregoing, your Affiant respectfully submits that there is probable cause to believe that Title 18 United States Code, Section 2252A(a)(2) and Title 18 United States Code, Section 2252A(a)(5)(B) have been violated and that there is probable cause to believe that evidence of these crimes can be found on the computer, hard drives, various DVDs and CDs, and cell phone seized at the SUBJECT PREMISES and more particularly described in Attachment A.

19. In consideration of the foregoing, I respectfully request that this Court issue a search warrant to search the items described in Attachments A which is incorporated herein by reference, and to seize any items located pursuant to the search as described in Attachment B, which is incorporated herein by reference.

Augustus Aquino
Special Agent, Homeland Security Investigations

Subscribed to and sworn before
me this 2ND day of October 2017.

The Honorable Beth P. Gesner
United States Magistrate Judge

17-2668 BPG

ATTACHMENT A

DESCRIPTION OF ITEMS TO BE SEARCHED

The evidence currently in the custody of HSI at to be searched is more particularly described as:

Compaq Presario Desktop Computer S/N 3CR8250FTF

Western Digital Hard Drive S/N WMAHN1018954

Western Digital Hard Drive S/N WCAC81735651

Western Digital Hard Drive S/N WMAD1A412255

Western Digital Hard Drive S/N WCASY9063502

Western Digital Hard Drive S/N WCAJA1002849

Western Digital Hard Drive S/N WMAD1A406698

Western Digital Hard Drive S/N WCADY1271986

Western Digital Hard Drive S/N WMAL71332618

Western Digital Hard Drive S/N WCAAT7278284

Western Digital Hard Drive S/N WMASY1516298

Quantum Hard Drive S/N 352068920250

Maxtor Hard Drive S/N A30H70LL

403 DVDs/CDs

Samsung Flip Phone Model #SCHU360

17-2668 BPG

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

1. All records, documentation, images, videos, or other data contained in the items described in Attachment A, including the following items to be seized which constitute evidence of violations of Title 18 U.S.C. § 2252A:

a. Any and all notes, documents, records, images, videos, text messages, correspondence, calendar entries, or other files referencing or depicting any minor engaged in sexually explicit conduct.

b. Any and all visual depictions of other minors engaged in sexually explicit conduct.

c. Any and all correspondence, computer files, or other data identifying persons transmitting, receiving or possessing, through interstate commerce including by computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18 U.S.C. § 2256(2).

d. Any and all diaries, notebooks, notes, and any other records reflecting personal contact with or communications about any minor.

e. Any and all records relating to persuading, inducing, enticing or coercing a minor to engage in any sexual activity in violation of the law.

f. Evidence indicating the user's state of mind as it relates to the crime under investigation within this warrant.

h. Evidence of user attribution showing who used or owned the electronic devices described in Attachment A or any predecessor devices replaced by the devices

described in Attachment A at the time the things described in this warrant were produced, created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

Any of the items described in paragraph 1 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment, including floppy diskettes, fixed hard disks, or removable hard disk cartridges, software or memory in any form. The search procedure of the electronic data contained in computer operating software or memory devices shall include the following techniques which shall be used to minimize the risk that those conducting the search will view information not within the scope of the warrant:

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
c. "scanning" storage areas to discover and possible recover recently deleted files;
d. "scanning" storage areas for deliberately hidden files; or
e. performing key word or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

2. If after performing these procedures, the directories, files or storage areas do not reveal evidence of child pornography or other criminal activity, the further search of that particular directory, file or storage area, shall cease.

17-2668 BPG

EXHIBIT A

SEARCH AND SEIZURE WARRANT

STATE OF MARYLAND

TO: Corporal Roger Schwarb #5774 , Maryland State Police, or/any other Law Enforcement Officer:

An APPLICATION for a Search and Seizure Warrant having been made before me by ***Corporal Roger Schwarb*** #5774, Maryland State Police;

AND it appears to me, from the Application and Affidavit (s) and any attachment(s) incorporated in it, that Probable Cause exists to believe that on or in the following described premises to wit: **50 North Drive, Earleville, Cecil County, Maryland 21919**

More particularly described as:

There is now being concealed/contained/secreted certain evidence in the premises to wit; evidence relating to the crimes of Possession and Distribution of Child Pornography, including but not limited to all instrumentalities of said crimes.

AND I am satisfied that the laws relating to:

Child Pornography, specifically:

Criminal Law, Section CR 11-208
Criminal Law, Section CR 11-207

of the Annotated Code of Maryland, as amended and revised are being/have been violated.

NOW, THEREFORE, pursuant to the provisions of Criminal Procedure, Section 1-203 of the Annotated Code of Maryland, as amended and revised, you are authorized to:

1. Enter and search the residence as completely described above for evidence of the aforementioned crime(s), to include evidence of Child Pornography and/or Sexual Child Exploitation.

2. Seize, preview and examine any cell phones that may have been used while acquiring Child Pornography and/or engaging Sexual Child Exploitation.

3. Seize, preview and examine any and all magnetic media not limited to Jaz discs, hard drives, floppy discs, or Zip drives. Any PCMCIA drives, Bernoulli discs or tapes of any type that may contain evidence, production, distribution, receipt, transmission, or viewing that may have been used while acquiring Child Pornography and/or engaging Sexual Child Exploitation.

4. Seize, preview and examine any Optical media to include but not limited to CD Rom, CDR, CDR-W, DVD, DVD-Rom or optical discs that may have been used while acquiring Child Pornography and/or engaging Sexual Child Exploitation.

5. Seize, preview and examine any computer hardware capable of analyzing, collecting, displaying, receiving, or transmitting data electrically, magnetically or optically. Hardware includes but is not limited to desktop computers, portable computers (I.E. laptops, IPADS, tablets), file servers, peripheral input/output devices (I.E. key boards, plotters, pointing devices, printers, scanners, and video display monitors), storage devices capable of reading and/or writing to computer media (I.E. electric, magnetic, optical), communication devices (I.E. modems, cable modems, network adapters and wireless communication devices), any device or parts used to restrict access to computer hardware (I.E. keys, locks), and any other piece of equipment necessary to duplicate the function of hardware at the time of seizure (I.E. batteries, cables, instruction manuals, power cords) that may have been used while acquiring Child Pornography and/or engaging Sexual Child Exploitation.

6. Search the following locations about the residence described above to include but not limited to; any outbuildings, locked or unlocked safes, any vehicles located on the property at the time of the search registered to or in the control of people at the residence, for evidence of the aforementioned crimes, to include evidence of Child Pornography.

7. Seize, preview and examine any and all electronic data processing and computer data storage devices, including; central processing units, internal and peripheral storage devices such as fixed disks, external hard disks, logged in e-mail accounts, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, optical readers and scanning devices, CD Rom drives and compact disks and related hardware, digital cameras and digital storage media devices (I.E. thumb drives), operating logs, software and operating instructions or operating manuals, computer manuals, software and programs used to communicate with other terminals via telephone or other means, and any computer modems, monitors, printers, etc that may have been used while acquiring Child Pornography and/or engaging Sexual Child Exploitation, as defined in the Annotated Code of Maryland, amended and revised;

8. Seize any photographs, magazines, motion pictures, videotapes, books, slides, drawings, negatives, undeveloped film or other items related to sexual abuse of children, child pornography or co-conspirators in the distribution, production, possession of Child Pornography and/or Sexual Child Exploitation.

9. Seize documents and effects which tend to show dominion and control over said location, including fingerprints, clothing, handwritings, documents and effects which bear a form of identification such as a person's name, address, photograph, Social Security number or driver's license number.

10. Search for any logs and any onsite computer network storage used by the suspect which may contain evidence pertaining to network computer traffic conducted by the user in the perpetration of the aforementioned crimes.

11. Search for passwords and data security devices. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. A password (string of alphanumeric characters) usually operates as a sort of digital key to unlock particular data security device(s). Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it. These items will be seized in order to facilitate the search of the computer systems/computer system components/computer systems storage media named above.

12. Open any containers, envelopes, boxes, packages, or safes to examine the contents and seize any of the aforementioned items.

13. Leave a copy of this warrant with an inventory of the property seized and return this warrant with an inventory, if any, to you within ten (10) days after the execution of this warrant for further disposition.

Subscribed and sworn to, this 8th day of August in the year 2017.

JUDGE